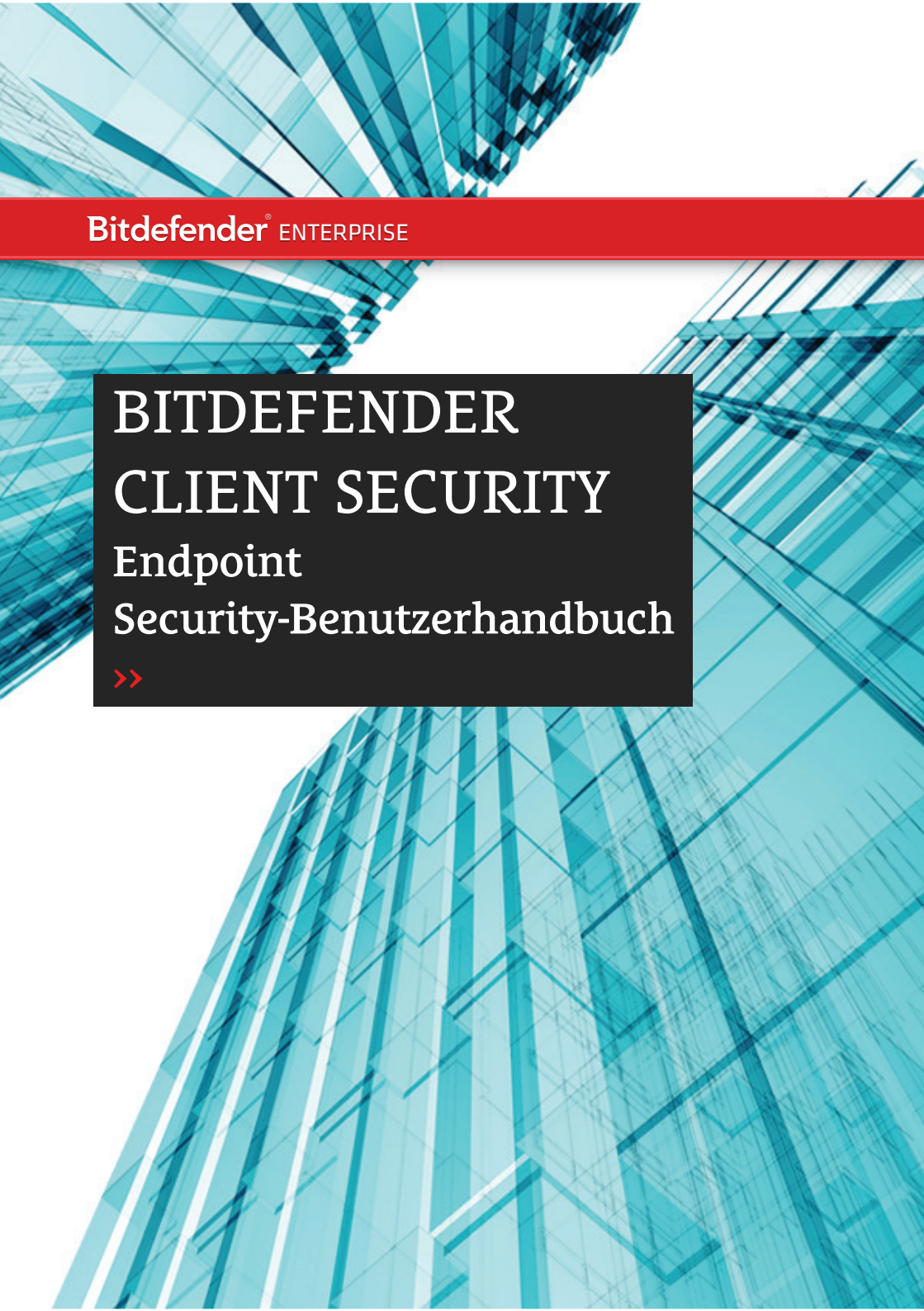

Bitdefender ENTERPRISE
BITDEFENDER
CLIENT SECURITY
Endpoint
Security-Benutzerhandbuch
>>

Bitdefender Client Security
Endpoint Security-Benutzerhandbuch

Veröffentlicht 2013.05.29

Copyright© 2013 Bitdefender

Rechtlicher Hinweis

Alle Rechte vorbehalten. Bestandteile dieses Handbuches dürfen weder in elektronischer noch mechanischer Form reproduziert werden. Dies gilt auch für das Fotokopieren, Aufnehmen oder jegliche andere Form von Datenspeicherung oder Informationsbeschaffung, ohne die Zustimmung von Bitdefender. Ausnahmen gelten für Zitate in Verbindung mit Testberichten. Der Inhalt darf in keiner Weise verändert werden.

Warnung und Haftungsausschluss. Dieses Produkt und die dazugehörige Dokumentation ist urheberrechtlich geschützt. Die Informationen in diesem Dokument werden „wie besehen" zur Verfügung gestellt und enthalten keinen Garantieanspruch. Obwohl dieses Dokument mit äußerster Sorgfalt erstellt und geprüft wurde, übernehmen die Autoren keinerlei Haftung für tatsächlich oder angeblich auftretende Schäden bzw. Datenverluste, die direkt oder indirekt durch die Informationen in diesem Dokumente entstehen könnten oder bereits entstanden sind.

Dieses Handbuch enthält Verweise auf andere, nicht von BITDEFENDER erstellte Webseiten, die auch nicht von BITDEFENDER kontrolliert werden. Somit übernimmt BITDEFENDER auch keine Verantwortung in jeglicher Art für den Inhalt dieser Webseiten. Der Besuch dieser Webseiten erfolgt somit auf eigene Gefahr. BITDEFENDER stellt diese Verweise aus Gründen der Anwenderfreundlichkeit zur Verfügung, was nicht bedeutet, dass BITDEFENDER in jeglicher Art und Weise Verantwortung oder Haftung für diese Webseiten und deren Inhalt übernimmt.

Warenzeichen. Es erscheinen eingetragene Warenzeichen in diesem Dokument. Alle eingetragenen und nicht eingetragenen Warenzeichen in diesem Dokument sind das alleinige Eigentum der jeweiligen Besitzer.

Bitdefender

Inhaltsverzeichnis

Zur Verwendung dieses Handbuchs v
1. Zielsetzung und Zielgruppe v
2. Über dieses Handbuch v
3. Konventionen in diesem Handbuch v
4. Ihre Mithilfe vi

1. Erste Schritte 1
1.1. System Tray Icon 1
1.2. Öffnen des Hauptfensters 2
1.3. Hauptfenster 2
1.3.1. Infobereich 4
1.3.2. Tafelbereich 4
1.4. Surf-Schutz 5
1.4.1. BitDefender Toolbar 5
1.4.2. Suchberater 6
1.4.3. Gesperrte Webseiten 6
1.5. Geräte-Scan 6
1.6. Anpassen von Schutzeinstellungen 7

2. Prüfung auf Malware 8
2.1. Scannen von Dateien und Ordnern 8
2.2. Durchführen von Quick Scans 8
2.3. Ausführen eines vollständigen System-Scans 9
2.4. Konfigurieren und Ausführen eines benutzerdefinierten Scans 9
2.5. Antivirus Prüfassistent 12
2.5.1. Schritt 1 - Führen Sie den Scan durch 12
2.5.2. Schritt 2 - Wählen Sie entsprechende Aktionen aus 13
2.5.3. Schritt 3 - Zusammenfassung 14
2.6. Scan-Protokolle werden überprüft 15

3. Updates 16
3.1. Arten von Updates 16
3.2. Überprüft, ob Ihr Schutz auf dem neuesten Stand ist 17
3.3. Durchführung eines Updates 17
3.4. Wobei handelt es sich bei der Frequenz für automatische Updates? 17

4. Die Quarantäne verwalten 18
4.1. Dateien in der Quarantäne anzeigen 18
4.2. Dateien in der Quarantäne löschen 18
4.3. Dateien aus der Quarantäne wiederherstellen 18

5. Ereignisanzeige 19

6. Hilfe erhalten 20

Zur Verwendung dieses Handbuchs

1. Zielsetzung und Zielgruppe

Diese Dokumentation richtet sich an die Endanwender von **Endpoint Security**, der Bitdefender-Client-Software, die auf Computern und Servern installiert wird, um diese vor Malware und anderen Bedrohungen aus dem Internet zu schützen und die Einhaltung von Richtlinien für die Benutzerkontrolle sicherzustellen.

Die hier bereitgestellten Informationen sollten für jeden Benutzer mit Erfahrung im Umgang mit Windows verständlich sein.

Viel Spaß mit diesen nützlichen und informativen Handbuch.

2. Über dieses Handbuch

Dieses Handbuch ist übersichtlich gestaltet, damit Sie im Handumdrehen alle benötigten Informationen finden können.

„Erste Schritte“ (S. 1)
Machen Sie sich mit der Endpoint Security-Benutzeroberfläche vertraut.

„Prüfung auf Malware“ (S. 8)
Erfahren Sie, wie Sie Malware-Scans ausführen können.

„Updates“ (S. 16)
Erfahren Sie mehr über Endpoint Security-Updates.

„Ereignisanzeige“ (S. 19)
Überprüfen Sie die Aktivität von Endpoint Security.

„Hilfe erhalten“ (S. 20)
Beschreibt wie Sie Hilfe bzw. Unterstützung zu dem Produkt erhalten und erhält zusätzlich eine Liste mit den am häufigsten gestellten Fragen (FAQ).

3. Konventionen in diesem Handbuch

Typografie

Zur Verbesserung der Lesbarkeit werden in diesem Handbuch verschiedene Textformate verwendet. Die Bedeutung der verschiedenen Formate können Sie der unten stehenden Tabelle entnehmen.

Erscheinungsbild	Beschreibung
documentation@bitdefender.com	Verweise auf E-Mail-Adressen, z.B. zur Kontaktaufnahme.
„Zur Verwendung dieses Handbuchs“ (S. v)	Interne Verweise (Links) auf beliebige Stellen innerhalb dieses Dokuments.
`Dateiname`	Dateien und Verzeichnisse werden in einer Schriftart mit `fester Laufweite` angegeben.
Option	Alle Produktoptionen werden **fett gedruckt** dargestellt.
Stichwort	Wichtige Stichwörter oder Begriffe werden durch **Fettdruck** hervorgehoben.

Symbole

Bei diesen Symbolen handelt es sich um Hinweise innerhalb des Textflusses welche mit einer kleinen Grafik markiert sind. Hierbei handelt es sich um Informationen die Sie in jedem Fall beachten sollten.

Beachten Sie

Diese Bemerkung dient lediglich zur Überprüfung. Notizen enthalten nützliche Informationen wie zum Beispiel einen Verweis auf ein verwandtes Thema.

Wichtig

Diese Art von Hinweis sollte in jedem Fall gelesen werden. Es werden signifikante Informationen zum jeweiligen Thema bereitgestellt. Es wird nicht empfohlen diese zu übergehen.

4. Ihre Mithilfe

Wir laden Sie dazu ein uns bei der Verbesserung dieses Dokuments mitzuhelfen. Wir haben sämtliche Informationen in diesem Dokument bestmöglich überprüft um somit die Qualität sicherzustellen.

Falls Sie dennoch Fehler finden, so teilen Sie uns diese bitte mit indem Sie uns per E-Mail unter der Adresse documentation@bitdefender.com kontaktieren.Bitte verfassen Sie bitte alle auf die Dokumentation bezogenen E-Mails auf Englisch.

1. Erste Schritte

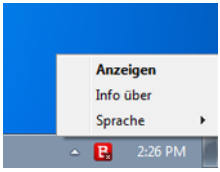
Endpoint Security ist eine vollständig automatisiertes Computer-Sicherheitslösung, die per Fernzugriff von Ihrem Netzwerkadministrator verwaltet wird. Nach der Installation schützt sie Sie vor allen Arten von Schad-Software (wie Viren, Spyware und Trojaner), Netzwerkangriffen, Phishing-Versuchen und Datendiebstahl. Zudem kann sie genutzt werden, um die Einhaltung von Unternehmensrichtlinien zur Computer- und Internet-Nutzung sicherzustellen.

Endpoint Security trifft alle sicherheitsrelevanten Entscheidungen für Sie und wird nur in seltenen Fällen Pop-up-Benachrichtigungen anzeigen.Nähere Informationen zu den durchgeführten Aktionen und zur Programmausführung finden Sie im Ereignisfenster.Für weitere Informationen lesen Sie bitte „Ereignisanzeige“ (S. 19).

1.1. System Tray Icon

Nach der Installation wird ein Endpoint Security-Symbol dauerhaft in Ihrer Task-Leiste angezeigt.Ein Doppelklick auf dieses Symbol öffnet das Hauptfenster des Programms. Mit einem Rechtsklick auf das Symbol öffnen Sie ein Kontextmenü mit nützlichen Optionen.

- **Anzeigen** - Öffnet das Endpoint Security-Hauptfenster.
- **Über** - öffnet ein Fenster, in dem Sie Informationen über Endpoint Security erhalten und Hilfe finden, falls etwas Unvorhergesehenes geschieht.Wenn Sie das Fenster öffnen, wird dadurch automatisch ein Bedarf-Update gestartet.
- **Sprache** - hier können Sie die Sprache der Benutzeroberfläche einstellen.



System Tray Icon

Das Bitdefender-Symbol in der Task-Leiste weist Sie auf Probleme hin, die Ihren Computer beeinträchtigen, indem es sein Aussehen verändert:

Kritische Probleme beeinträchtigen die Sicherheit Ihres Systems.

Nicht-kritische Probleme beeinträchtigen die Sicherheit Ihres Systems.

Beachten Sie

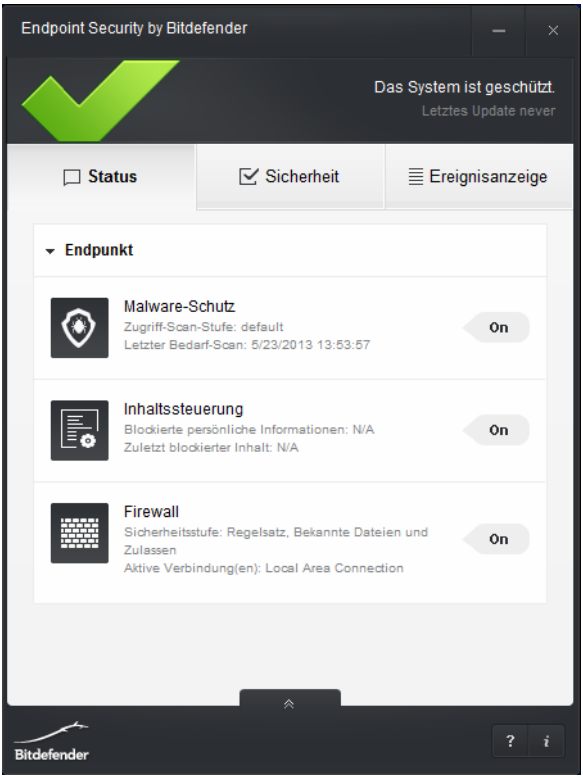
Der Netzwerkadministrator kann das Taskleistensymbol ausblenden, wenn er möchte.

1.2. Öffnen des Hauptfensters

Sie können die Benutzeroberfläche von Endpoint Security aus dem Windows-Startmenü heraus über den folgenden Pfad aufrufen: **Start** → **Alle Programme** → **Endpoint Security by Bitdefender** → **Sicherheitskonsole öffnen**. Noch schneller geht es mit einem Doppelklick auf das Bitdefender-Symbol in der Task-Leiste.

1.3. Hauptfenster

Im Hauptfenster von Endpoint Security können Sie den Schutzstatus einsehen, Scan-Aufgaben durchführen und die Quarantäne verwalten. Und das alles mit nur wenigen Klicks.Die Konfiguration und Verwaltung der Sicherheit erfolgt per Fernzugriff durch Ihren Netzwerkadministrator.

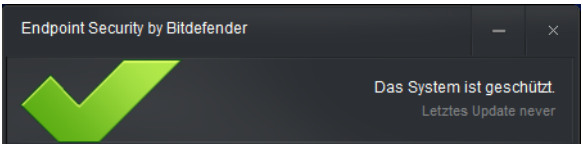


Hauptfenster

Das Fenster ist in zwei Hauptbereiche aufgeteilt:

Infobereich

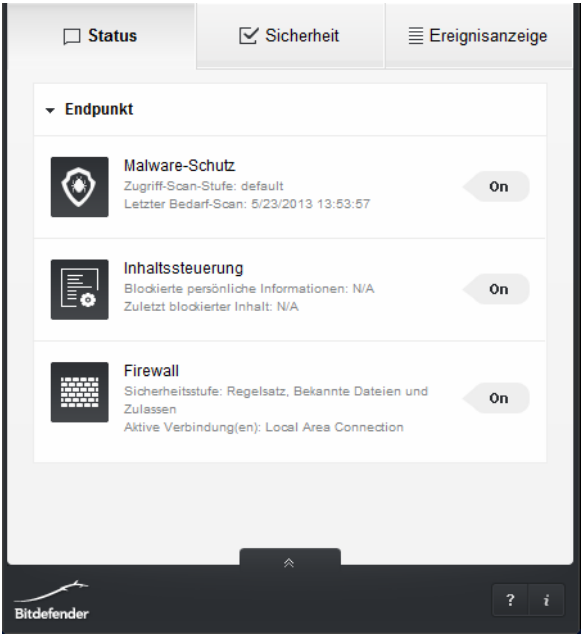
Hier können Sie den Sicherheitsstatus Ihres Computers überprüfen und sehen, welche Probleme die Sicherheit Ihres Systems gefährden.



Infobereich

Tafelbereich

In den Tafeln können Sie den Status jedes installierten Sicherheitsmoduls sehen, Bedarf-Scan-Aufgaben verwalten und die von Endpoint Security protokollierten Ereignisse sehen.



Tafelbereich

Zusätzlich finden Sie eine Reihe nützlicher Support-Optionen im unteren Bereich des Fensters:

Optionen	Beschreibung
?	Klicken Sie auf dieses Symbol, wenn Sie Hilfe mit Endpoint Security benötigen.
i	Klicken Sie auf dieses Symbol, um Produkt- und Kontaktinformationen anzuzeigen.

1.3.1. Infobereich

Im Infobereich finden Sie hilfreiche Informationen zur Sicherheit des Systems.

Sie können den aktuellen Sicherheitsstatus ganz leicht am Statussymbol links vom Infobereich ablesen:

- **Grünes Häkchen.** Es müssen keine Probleme behoben werden.Ihr Rechner und Ihre Daten sind geschützt.
- **Gelbes Ausrufezeichen.** Die Sicherheit Ihres Systems wird durch nicht-kritische Probleme beeinträchtigt.
- **Rotes Ausrufezeichen.** Die Sicherheit Ihres Systems wird durch kritische Probleme beeinträchtigt.

Zusätzlich zum Statussymbol wird ein Sicherheitsstatushinweis rechts vom Infobereich angezeigt.Sie können die gefundenen Sicherheitsprobleme anzeigen, indem Sie auf eine beliebige Stelle im Infobereich klicken.Bestehende Probleme werden von Ihrem Netzwerkadministrator behoben.

1.3.2. Tafelbereich

In den Tafeln können Sie den Status jedes installierten Sicherheitsmoduls sehen, Bedarf-Scan-Aufgaben verwalten und die von Endpoint Security protokollierten Ereignisse sehen.

In diesem Bereich stehen Ihnen die folgenden Tafeln zur Verfügung:

Status

Hier können Sie Einzelheiten zum Status und der Aktivität der installierten Sicherheitsmodule sehen.

- **Malware-Schutz.** Der Malware-Schutz bildet die Grundlage Ihrer Sicherheit. Endpoint Security schützt Sie sowohl in Echtzeit als auch bei Bedarf vor allen Arten von Malware, so zum Beispiel vor Viren, Trojanern, Spyware, Adware usw.
- **Firewall.** Die Firewall schützt Sie, wenn Sie mit Netzwerken und dem Internet verbunden sind, indem sie Verbindungsversuche filtert und verdächtigte oder gefährliche Verbindungen blockiert.

- **Inhaltssteuerung.** Das Modul Inhaltssteuerung schützt Sie im Internet vor Phishing-Angriffen, Betrugsversuchen, Diebstahl vertraulicher Daten und nicht jugendfreien Inhalten. Zudem enthält es umfangreiche Benutzerkontrollen, mit denen der Netzwerkadministrator die Einhaltung von Richtlinien zur Computer- und Internet-Nutzung sicherstellen kann.

Sicherheit

Hier können Sie System-Scans starten und die Quarantäne verwalten. Die folgenden Scan-Aufgaben stehen zur Auswahl:

- Beim **Quick Scan** wird das sog In-the-Cloud-Verfahren angewandt, um auf Ihrem System laufende Malware aufzuspüren.Die Ausführung eines Quick Scans dauert im Normalfall weniger als eine Minute und beansprucht nur einen Bruchteil der Systemressourcen, die ein normaler Virenscan in Anspruch nehmen würde.
- Der **Vollständige Scan** durchsucht den gesamten Computer nach allen Typen von Schad-Software, die ein Sicherheitsrisiko darstellen, so z. B. Viren, Spyware, Adware, Rootkits usw.
- **Benutzerdefinierter Scan** Hierbei können Sie die Bereiche, die gescannt werden sollen, selbst auswählen und die Scan-Optionen festlegen.

Weitere Informationen finden Sie unter „Prüfung auf Malware“ (S. 8).

Ereignisanzeige

Hier können Sie eine detaillierte Übersicht aller relevanten Ereignisse abrufen, die beim Betrieb des Produktes aufgetreten sind.Detaillierte Informationen finden Sie unter „Ereignisanzeige“ (S. 19).

1.4. Surf-Schutz

Ihr Bitdefender-Administrator kann Sicherheitseinstellungen festlegen, die sich auf Ihre Internet-Nutzung auswirken können. Diese Sicherheitseinstellungen betreffen unter anderem:

- „BitDefender Toolbar“ (S. 5)
- „Suchberater“ (S. 6)
- „Gesperrte Webseiten“ (S. 6)

1.4.1. BitDefender Toolbar

Falls Ihr Bitdefender-Administrator dies eingerichtet hat, informiert Sie die Bitdefender-Symbolleiste über die Sicherheitsbewertung der von Ihnen aufgerufenen Webseite. Die Bitdefender-Symbolleiste unterscheidet sich von anderen Browser-Symbolleisten, denn Sie fügt lediglich einen kleinen Dragger zu Ihrem Browser hinzu, der am oberen Rand jeder Webseite angezeigt wird. Mit einem Klick auf den Dragger öffnen Sie die Symbolleiste.

Je nachdem, wie Bitdefender die Webseite einstuft, wird eine der folgenden Nachrichten in der Symbolleiste angezeigt:

- "Diese Seite ist nicht sicher." wird neben einem roten Ausrufezeichen angezeigt.
- "Seien Sie vorsichtig" wird neben einem gelben Ausrufezeichen angezeigt.
- "Diese Seite ist sicher" wird neben einem grünen Häkchen angezeigt.

1.4.2. Suchberater

Falls der Suchberater von Ihrem Bitdefender-Administrator eingerichtet wurde, bewertet dieser sowohl die Suchergebnisse von Google, Bing und Yahoo! als auch Links auf Facebook und Twitter, indem es ein Symbol vor jedem Ergebnis platziert. Im Folgenden finden Sie die verwendeten Symbole und deren Bedeutung:

Sie sollten diese Webseite nicht aufrufen.

Diese Webseite könnte gefährliche Inhalte haben. Lassen Sie Vorsicht walten, wenn Sie sie dennoch aufrufen wollen.

Diese Seite konnte von Endpoint Security nicht verifiziert werden.

Diese Seite ist sicher.

1.4.3. Gesperrte Webseiten

Abhängig von den von Ihrem Bitdefender-Administrator festgelegten Sicherheitsrichtlinien wurden unter Umständen bestimmte Surf-Schutz-Einstellungen eingerichtet, die Phishing-Angriffe und Internet-Betrugsversuche verhindern sollen. Bitdefender blockiert unter Umständen automatisch bekannte Phishing-Seiten (gefälschte Webseiten), um zu verhindern, dass Sie versehentlich private oder vertrauliche Informationen an Online-Betrüger weitergeben. Neben gefälschten Webseiten können auch andere Formen von Internet-Betrug unterdrückt werden, so zum Beispiel: Verkaufsbetrug, Get-Rich-Quick-Betrug, Internet-Marketing-Betrug, Klick-Betrug, usw. Anstelle der schädlichen Webseite wird eine spezielle Warnseite angezeigt, die Sie über die Gefahren der aufgerufenen Webseite informiert.

Beachten Sie
Falls Sie eine unbedenkliche Webseite aufrufen möchten, die fälschlicherweise erkannt und blockiert wurde, wenden Sie sich bitte an Ihren Bitdefender-Administrator, damit dieser die Seite freigeben kann.

1.5. Geräte-Scan

Endpoint Security kann konfiguriert werden automatisch Speichermedien (CDs/DVDs, USB Speicher oder Netzlaufwerke) zu entdecken und Sie auffordern diese zu Prüfen oder nicht.Im Warnfenster werden Informationen über das erkannte Gerät angezeigt.

Um das Gerät zu prüfen, clicken Sie **Ja**.Wenn Sie sicher sind, dass das Gerät sauber ist, können Sie wählen es nicht zu prüfen.

Beachten Sie
Falls mehrere Geräte gleichzeitig erkannt werden, wird für jedes Gerät nacheinander ein eigenes Warnfenster angezeigt.

Ihr Bitdefender-Administrator kann Endpoint Security-Warnungen und -Benachrichtigungen auch unterdrücken.In diesen Fällen wird der Geräte-Scan automatisch gestartet, ohne dass Sie sich darum kümmern müssen.

Wenn ein Geräte-Scan ausgeführt wird, wird ein entsprechendes Symbol für den Scan-Fortschritt in der Task-Leiste angezeigt.Doppelklicken Sie auf dieses Symbol, um das Scan-Fenster zu öffnen und den Scan-Fortschritt anzuzeigen.Sie können den Geräte-Scan jederzeit anhalten oder beenden.Weitere Informationen finden Sie unter „Antivirus Prüfassistent“ (S. 12).

1.6. Anpassen von Schutzeinstellungen

Die Konfiguration und Verwaltung von Endpoint Security erfolgt per Fernzugriff durch Ihren Netzwerkadministrator.Sie können die Schutzeinstellungen nicht bearbeiten.

Sollten Sie Fragen zu Ihren Schutzeinstellungen haben, wenden Sie sich bitte an den für Ihre Netzwerksicherheit verantwortlichen Mitarbeiter.

2. Prüfung auf Malware

Die Hauptaufgabe von Endpoint Security ist es, Ihren Computer frei von Schad-Software zu halten. Dies geschieht vornehmlich durch Echtzeit-Scans aller aufgerufenen Dateien, E-Mail-Nachrichen und aller neuen Dateien, die auf Ihren Computer heruntergeladen oder kopiert werden. Neben dem Echtzeitschutz ist auch möglich, Scans auszuführen, um Schad-Software auf Ihrem Computer zu erkennen und zu entfernen.

Sie können den Computer jederzeit scannen, indem Sie die Standard-Aufgaben oder Ihre eigenen Scan-Aufgaben (benutzerdefinierte Aufgaben) ausführen.Die Scan-Aufgaben beinhalten die Scan-Optionen und die Objekte, die gescannt werden sollen.Wenn Sie bestimmte Bereiche Ihres Computers scannen oder die Scan-Optionen konfigurieren möchten, können Sie einen benutzerdefinierten Scan konfigurieren und ausführen.

2.1. Scannen von Dateien und Ordnern

Wenn Sie den Verdacht hegen, dass Dateien und Verzeichnisse infiziert sein könnten, sollten Sie einen Scan durchführen.Klicken Sie mit der rechten Maustaste auf die Datei oder den Ordner, die/den Sie scannen möchten, und wählen Sie **Mit Endpoint Security von Bitdefender scannen**.Der Antivirus Prüfassistent wird erscheinen und Sie durch den Prüfprozess führen.Wenn der Scan beendet wurde, werden Sie aufgefordert, die Aktionen auszuwählen, die für die infizierten Dateien ausgeführt werden sollen. Sie können auch entscheiden, keine Aktionen auszuführen.

2.2. Durchführen von Quick Scans

Beim Quick Scan wird das sog In-the-Cloud-Verfahren angewandt, um auf Ihrem System laufende Malware aufzuspüren.Die Ausführung eines Quick Scans dauert im Normalfall weniger als eine Minute und beansprucht nur einen Bruchteil der Systemressourcen, die ein normaler Virenscan in Anspruch nehmen würde.

Um einen Quick Scan auszuführen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Endpoint Security-Fenster.
2. Gehen Sie zur Tafel **Aufgaben**.
3. Klicken Sie auf **Scan** bei der Option **Quick Scan**.
4. Warten Sie, bis der Viren-Scan-Assistent den Scan abgeschlossen hat.Endpoint Security wird automatisch die empfohlenen Aktionen für die infizierten Dateien ausführen.Sollte es noch ungelöste Bedrohungen geben, werden Sie aufgefordert, die Aktionen auszuwählen, die durchgeführt werden sollen.

2.3. Ausführen eines vollständigen System-Scans

Der vollständige System-Scan scannt den gesamten Computer nach allen Malware-Typen, die ein Sicherheitsrisiko darstellen, so zum Beispiel Viren, Spyware, Adware, Rootkits usw.

Beachten Sie
Da ein **Vollständiger System-Scan** einen gründlichen Scan des gesamten Systems durchführt, kann dieser einige Zeit in Anspruch nehmen. Es empfiehlt sich daher, diese Aufgabe durchzuführen, wenn Sie den Computer nicht benötigen.

Wenn Sie bestimmte Bereiche Ihres Computers scannen oder die Scan-Optionen konfigurieren möchten, können Sie einen benutzerdefinierten Scan konfigurieren und ausführen.Für weitere Informationen lesen Sie bitte „Konfigurieren und Ausführen eines benutzerdefinierten Scans“ (S. 9).

Bevor Sie einen vollständigen System-Scan ausführen, sollten Sie Folgendes beachten:

- Stellen Sie sicher, dass die Malware-Signaturen von Endpoint Security immer auf dem neuesten Stand sind. Wenn Sie Ihren Computer auf Grundlage einer veralteten Signaturdatenbank scannen, könnte dies verhindern, dass Endpoint Security neue Malware erkennt, die seit dem letzten Update entdeckt wurde.Für weitere Informationen lesen Sie bitte „Updates“ (S. 16).
- Schließen Sie alle geöffneten Programme.

Um einen vollständigen System-Scan durchzuführen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Endpoint Security-Fenster.
2. Gehen Sie zur Tafel **Aufgaben**.
3. Klicken Sie auf **Scan** bei der Option **Vollständiger Scan**.
4. Warten Sie, bis der Viren-Scan-Assistent den Scan abgeschlossen hat.Endpoint Security wird automatisch die empfohlenen Aktionen für die infizierten Dateien ausführen.Sollte es noch ungelöste Bedrohungen geben, werden Sie aufgefordert, die Aktionen auszuwählen, die durchgeführt werden sollen.

2.4. Konfigurieren und Ausführen eines benutzerdefinierten Scans

Um einen Malware-Scan im Detail zu konfigurieren und dann auszuführen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Endpoint Security-Fenster.
2. Gehen Sie zur Tafel **Aufgaben**.
3. Klicken Sie auf **Neu** bei der Option **Benutzerdefinierter Scan**.

Ein neues Fenster wird sich öffnen.Folgen Sie diesen Schritten:

a. Sie können die Konfiguration einfach durch das Wählen der Scan-Tiefe festlegen. Ziehen Sie dazu den Zeiger an der Skala entlang, bis Sie den gewünschten Level erreicht haben.Die Beschreibung auf der rechten Seite der Skala helfen Ihnen, die Scan-Tiefe zu wählen, die für Ihre Bedürfnisse am besten geeignet ist.

   Erfahrene Benutzer können die Scan-Einstellungen von Endpoint Security nutzen.Um die Scan-Optionen im Detail zu konfigurieren, klicken Sie auf **Einstellungen**. Nach Auswahl Ihrer benutzerdefinierten Einstellungen wird der Scan-Status automatisch auf **Anpassen** gesetzt. Weitere Informationen zu den benutzerdefinierten Einstellungen finden Sie am Ende dieses Kapitels.

b. Sie können auch folgende allgemeine Optionen konfigurieren:

   - **Aufgabe mit niedriger Priorität ausführen .** Herabstufung der Priorität des Prüfvorgangs. Andere Programme werden somit schneller ausgeführt. Der gesamte Prüfvorgang dauert damit aber entsprechend länger.
   - **Scan-Assistent in die Task-Leiste minimieren .** Minimiert das Scan-Fenster in die Task-Leiste. Doppelklicken Sie auf das Symbol für den Scan-Fortschritt, um es wieder zu öffnen.

4. Klicken Sie auf **Weiter**, um die Orte zu wählen, die gescannt werden sollen.
5. Klicken Sie auf die **Hinzufügen**-Schaltfläche, um die Bereiche auszuwählen, die gescannt werden sollen. Wenn Sie die Einträge aus der Zielliste löschen möchten, klicken Sie auf die **Löschen**-Schaltfläche.
6. Klicken Sie auf **Weiter**, um den Scan zu starten, und warten Sie, bis der Viren-Scan-Assistent den Scan abgeschlossen hat.Abhängig von den Bereichen, die gescannt werden sollen, kann der Scan einige Zeit in Anspruch nehmen.Wenn der Scan beendet wurde, werden Sie aufgefordert, die Aktionen auszuwählen, die für die infizierten Dateien ausgeführt werden sollen. Sie können auch entscheiden, keine Aktionen auszuführen.

Informationen zu den Scan-Optionen

Diese Informationen sind vielleicht nützlich:

- Wenn Ihnen bestimmte Begriffe nicht geläufig sind, schlagen Sie diese im Glossar nach.Sie könne auch durch eine Suche im Internet hilfreiche Informationen finden.
- **Dateitypen.** Sie können Endpoint Security so einstellen, dass alle Dateitypen oder nur Anwendungen (Programmdateien) gescannt werden.Das Scannen aller Dateien bietet den besten Schutz, während das Scannen nur von Anwendungen verwendet wird, um einen schnelleren Scan durchzuführen.

  Anwendungen (oder Programmdateien) sind weitaus anfälliger für Malware-Angriffe als andere Dateitypen.Diese Kategorie beinhaltet die folgenden Dateierweiterungen:`386;`

a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

- **Scan-Optionen für Archive.** Archive mit infizierten Dateien sind keine unmittelbare Bedrohung für Ihre Systemsicherheit.Die Malware kann Ihr System nur beeinflussen, wenn die infizierten Datei aus einem Archiv extrahiert und ohne aktivierten Echtzeitschutz ausgeführt wird.Wir empfehlen jedoch, diese Option zu nutzen, um jegliche potentiellen Bedrohungen aufzuspüren und zu entfernen, auch wenn es sich nicht um unmittelbare Bedrohungen handelt.

  Beachten Sie
  Das Scannen archivierter Dateien erhöht die Gesamt-Scandauer und erfordert mehr Systemressourcen.

- **Boot-Sektoren scannen.** Sie können Endpoint Security einstellen, damit die Boot-Sektoren gescannt werden.Dieser Sektor der Festplatte beinhaltet den notwendigen Computercode um den Boot-Prozess zu starten.Wenn ein Virus den Boot-Sektor infiziert, könnte das Laufwerk unzugänglich werden und es könnte Ihnen nicht mehr möglich sein, Ihr System zu starten und auf Ihre Daten zuzugreifen.
- **Nach Rootkits suchen.** Wählen Sie diese Option, um nach Rootkits und Objekten zu suchen, die mit dieser Art von Software versteckt werden.
- **Speicher scannen.** Wählen Sie diese Option, um Programme zu scannen, die im Speicher Ihres Systems laufen.
- **Registry scannen.** Wählen Sie diese Option, um die Registry-Schlüssel zu scannen.Die Windows-Registry ist eine Datenbank, in der Konfigurationseinstellungen und Optionen für die Windows-Betriebssystemkomponenten sowie für die installierten Anwendungen gespeichert sind.

- **Cookies prüfen.** Wählen Sie diese Option, um die Cookies zu scannen, die von Ihrem Browser auf Ihrem Computer gespeichert werden.
- **Nur neue und geänderte Dateien.** Indem nur neue und geänderte Dateien gescannt werden, können Sie die allgemeine Systemreaktionsfähigkeit mit minimalen Sicherheitsabstrichen erheblich verbessern.
- **Kommerzielle Keylogger ignorieren.** Wählen Sie diese Option, wenn Sie auf Ihrem Computer eine kommerzielle Keylogger-Software nutzen.Kommerzielle Keylogger sind seriöse Programme zur Überwachung des Computers, deren Hauptfunktion es ist, alle Tastatureingaben aufzuzeichnen.

2.5. Antivirus Prüfassistent

Der Endpoint Security-Viren-Scan-Assistent erscheint, sobald Sie einen Bedarf-Scan starten (zum Beispiel, indem Sie mit der rechten Maustaste auf einen Ordner klicken und dann **Mit Endpoint Security von Bitdefender scannen** auswählen).Folgen Sie den Anweisungen des Assistenten, um den Scan-Prozess abzuschließen.

Beachten Sie

Falls der Prüfassistent nicht erscheint, ist die Prüfung möglicherweise konfiguriert still, im Hintergrund, zu laufen.Achten Sie auf das Symbol für den Scan-Fortschritt in der Task-Leiste.Doppelklicken Sie auf dieses Symbol, um das Scan-Fenster zu öffnen und den Scan-Fortschritt anzuzeigen.

2.5.1. Schritt 1 - Führen Sie den Scan durch

Endpoint Security startet den Scan der aus gewählten Dateien und Verzeichnisse.Sie erhalten Echtzeitinformationen über den Scan-Status sowie Scan-Statistiken (einschließlich der bisherigen Laufzeit, einer Einschätzung der verbleibenden Laufzeit und der Anzahl der erkannten Bedrohungen).Klicken Sie auf **Mehr anzeigen**, um weitere Details zu erhalten.

Bitte warten Sie, bis der Scan abgeschlossen ist.Der Prüfvorgang kann, abhängig von der Größe Ihrer Festplatte, einen Moment dauern.

Stoppen oder pausieren der Prüfung. Sie können die Prüfung jederzeit beenden, indem Sie auf **Abbrechen** klicken. Dadurch gelangen Sie direkt zum letzten Schritt des Assistenten.Um den Prüfvorgang vorrübergehend zu stoppen klicken Sie einfach auf **Pause**. Um den Prüfvorgang fortzusetzen klicken Sie auf **Fortsetzen** .

Passwortgeschützte Archive. Wird ein passwortgeschütztes Archiv gefunden, werden Sie, abhängig von den Scan-Einstellungen, um die Eingabe des Passwortes gebeten.Mit Passwörtern geschützte Archive können nicht geprüft werden, außer wenn Sie das Passwort angeben.Die folgenden Optionen sind verfügbar:

- **Passwort.** Wenn Sie möchten, dass Endpoint Security Archive scannt, wählen Sie diese Option aus und geben das Passwort an.Falls Sie das Passwort nicht kennen, wählen Sie eine der anderen Optionen.
- **Nicht nach Passwort fragen; das Objekt beim Scan überspringen.** Wählen Sie diese Optione um das Prüfen diesen Archivs zu überspringen.
- **Alle Passwortgeschützte Datein überspringen ohne diese zu Prüfen.** Wählen Sie diese Option, falls Sie nicht über passwortgeschützte Archive informiert werden möchten.Endpoint Security kann diese Dateien und Objekte nicht scannen, erstellt aber einen Eintrag im Scan-Protokoll.

Wählen Sie die gewünschte Option aus und klicken Sie auf **OK**, um den Scan fortzusetzen.

2.5.2. Schritt 2 - Wählen Sie entsprechende Aktionen aus

Wenn der Scan beendet wurde, werden Sie aufgefordert, die Aktionen auszuwählen, die für die infizierten Dateien ausgeführt werden sollen. Sie können auch entscheiden, keine Aktionen auszuführen.

Beachten Sie

Wenn Sie einen Quick Scan oder einen vollständigen System-Scan durchführen, wird Endpoint Security während des Scans automatisch die empfohlenen Aktionen für die infizierten Dateien ausführen.Sollte es noch ungelöste Bedrohungen geben, werden Sie aufgefordert, die Aktionen auszuwählen, die durchgeführt werden sollen.

Die infizierten Objekte werden in Gruppen angezeigt, je nach Malware, mit der sie infiziert sind.Klicken Sie auf den Link, der der Bedrohung entspricht, um weitere Informationen über die infizierten Objekte zu erhalten.

Sie können eine umfassende Aktion für alle Probleme auswählen oder Sie können einzelne Aktionen für Problemgruppen auswählen.Eine oder mehrere der folgenden Optionen können im Menu erscheinen:

Aktionen ausführen

Endpoint Security wird je nach Art der infizierten Datei die empfohlenen Aktionen ausführen:

- **Infizierte Dateien.** Als infiziert erkannte Dateien stimmen mit einer Malware-Signatur in der Bitdefender-Malware-Signatur-Datenbank überein.Endpoint Security wird automatisch versuchen, den Malware-Code aus der infizierten Datei zu entfernen und die Originaldatei zu rekonstruieren.Diese Operation bezeichnet man als Desinfektion.

  Dateien, die nicht desinfiziert werden können, werden in die Quarantäne verschoben, um so die Infizierung einzudämmen.Dateien in der Quarantäne können nicht ausgeführt oder geöffnet werden; aus diesem Grund besteht kein Infektionsrisiko?

Wichtig
Bestimmte Malware-Typen können nicht desinfiziert werden, da die komplette Datei betroffen ist. In diesen Fällen wird die infizierte Datei von der Festplatte gelöscht.

- **Verdächtige Dateien.** Dateien werden von der heuristischen Analyse als verdächtig klassifiziert.Verdächtige Dateien können nicht desinfiziert werden, da hierfür keine Desinfektionsroutine verfügbar ist. Sie werden in Quarantäne verschoben, um eine mögliche Infektion zu verhindern.

  Dateien in Quarantäne werden standardmäßig an die Bitdefender-Labore geschickt, damit Sie dort von den Bitdefender-Malware-Forschern analysiert werden können.Sollten das Vorhandensein von Malware bestätigt werden, wird eine Signatur veröffentlicht, um das Entfernen der Malware zu ermöglichen.

- **Archive mit infizierten Dateien.**
  - Archive, die nur infizierte Dateien enthalten, werden automatisch gelöscht.
  - Wenn ein Archiv sowohl infizierte als auch nicht infizierte Dateien enthält, wird Endpoint Security versuchen, die infizierten Dateien zu löschen, vorausgesetzt, dass das Archiv mit den nicht infizierten Dateien wieder rekonstruiert werden kann.Wenn das Archiv nicht rekonstruiert werden kann, werden Sie benachrichtigt, dass keine Aktion durchgeführt werden kann, weil die Gefahr besteht, dass nicht infizierte Dateien verloren gehen.

Löschen
Infizierte Dateien werden von der Festplatte entfernt.

Falls infizierte Dateien zusammen mit nicht infizierten Dateien in einem Archiv gespeichert sind, wird Endpoint Security versuchen, die infizierten Dateien zu löschen und das Archiv mit den nicht infizierten Dateien zu rekonstruieren.Wenn das Archiv nicht rekonstruiert werden kann, werden Sie benachrichtigt, dass keine Aktion durchgeführt werden kann, weil die Gefahr besteht, dass nicht infizierte Dateien verloren gehen.

Ignorieren
Es wird keine Aktion für die infizierte Dateien ausgeführt.Nachdem der Prüfvorgang beendet wurde, können Sie das Prüfprotokoll öffnen um Informationen über diese Dateien zu betrachten.

Klicken Sie auf **Fortfahren** um die festgelegten Aktionen anzuwenden.

2.5.3. Schritt 3 - Zusammenfassung

Wenn Endpoint Security die Probleme gelöst hat, wird eine Zusammenfassung der Scan-Ergebnisse in einem neuen Fenster angezeigt.Falls Sie umfangreichere Informationen zum Scan-Prozess möchten, klicken Sie auf **Logdatei anzeigen**.

Klicken Sie auf **Schließen** um dieses Fenster zu schließen.

Wichtig

In den meisten Fällen desinfiziert Endpoint Security erfolgreich die aufgespürten infizierten Dateien oder er isoliert die Infektion.Dennoch gibt es Probleme, die nicht automatisch gelöst werden können.Bitte starten Sie Ihr System neu, wenn Sie dazu aufgefordert werden, damit der Säuberungsprozess abgeschlossen werden kann.

2.6. Scan-Protokolle werden überprüft

Für jeden Scan wird ein Protokoll erstellt.Der Bericht enthält detaillierte Informationen über den Prüfprozess, so wie Prüfoptionen, das Prüfziel, die entdeckten Bedrohungen und die Aktionen, die für diese Bedrohungen ausgeführt wurden.

Sobald der Scan beendet ist, können Sie das Scan-Protokoll direkt aus dem Scan-Assistenten heraus öffnen, indem Sie auf **Protokoll anzeigen** klicken.

Um die Scan-Protokolle zu einem späteren Zeitpunkt zu überprüfen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Endpoint Security-Fenster.
2. Gehen Sie zur Tafel **Ereignisse**.
3. Wählen Sie **Malware-Schutz** im zweiten Menü.Hier können Sie alle Malware-Scan-Ereignisse finden, einschließlich der Bedrohungen, die während Zugriff-Scans und vom Benutzer gestarteten Scans entdeckt wurden. Dazu kommen Statusänderungen für automatische Scans.
4. In der Ereignisliste können Sie überprüfen, welche Scans kürzlich durchgeführt wurden.Klicken Sie auf ein Ereignis, um mehr darüber zu erfahren.
5. Sie können das Scan-Protokoll öffnen, indem Sie auf den Ort klicken, der im Detailbereich unten auf der Tafel angegeben ist.Das Scan-Protokoll wird angezeigt.

3. Updates

In einer Welt, in der Internet-Kriminelle immer neue Wege finden, um Ihnen zu schaden, ist es von größter Wichtigkeit, dass Sie Ihre Sicherheitslösung zu jeder Zeit auf dem neuesten Stand halten, um stets einen Schritt voraus zu sein.

Falls Sie über eine Breitbandverbindung oder eine DSL-Verbindung mit dem Internet verbunden sind, arbeitet die Endpoint Security-Software eigenständig. Sie überprüft zunächst beim Start des Computers und danach **stündlich**, ob neue Updates verfügbar sind.Wenn ein neues Update erkannt wird, wird es automatisch auf Ihren PC heruntergeladen und installiert.

Beachten Sie

Die standardmäßige Frequenz für automatische Updates kann von Ihrem Netzwerkadministrator angepasst werden.Für weitere Informationen lesen Sie bitte „Wobei handelt es sich bei der Frequenz für automatische Updates?“ (S. 17).

Der Update-Vorgang wird "on-the-fly" durchgeführt. Das bedeutet, dass die Dateien, die aktualisiert werden sollen, nach und nach ersetzt werden. Dadurch wird die Funktionalität des Produkts nicht eingeschränkt und Ihr System wird nicht gefährdet.

Falls Sie über eine Internetverbindung per Einwahl verfügen, ist es sinnvoll, regelmäßig ein manuelles BitDefender-Update durchzuführen. Für weitere Informationen lesen Sie bitte „Durchführung eines Updates“ (S. 17).

3.1. Arten von Updates

Folgende Update-Möglichkeiten stehen zur Verfügung:

- **Updates der Malware-Signaturen** - Immer wenn neue Bedrohungen auftreten, müssen die Dateien mit den Malware-Signaturen aktualisiert werden, um einen durchgängigen und aktuellen Schutz zu gewährleisten.
- **Produkt-Updates** - wenn eine neue Version auf dem Markt erscheint, enthält diese zur Leistungssteigerung des Produkts neue Funktionen und Scantechniken.

  Bei einem Produkt-Upgrade handelt es sich um eine neue Hauptversion der Software.

3.2. Überprüft, ob Ihr Schutz auf dem neuesten Stand ist

Um zu überprüfen, ob Ihr Schutz auf dem neuesten Stand ist, gehen Sie folgendermaßen vor:

1. Klicken Sie mit der rechten Maustaste auf das Bitdefender-Symbol in der Task-Leiste und wählen Sie danach **Über**.
2. Der Update-Status und der Zeitpunkt der letzten Update-Überprüfung und Update-Installation werden angezeigt.

Um ausführliche Informationen zu Ihren letzten Updates zu erhalten, rufen Sie die Update-Ereignisse auf:

1. Gehen Sie im Hauptfenster zur Tafel **Ereignisse**.
2. Klicken Sie im zweiten Menü auf **Update**.

Sie können herausfinden, wann Updates angestoßen wurden und weitere Informationen dazu einholen (d.h. ob sie erfolgreich waren oder nicht, ob ein Neustart erforderlich ist, um die Installation abzuschließen).Falls nötig starten Sie das System sobald es Ihnen möglich ist neu.

3.3. Durchführung eines Updates

Sie benötigen eine Internet-Verbindung, um Updates durchzuführen.

Klicken Sie mit der rechten Maustaste auf das Bitdefender-Symbol in der Task-Leiste und wählen Sie danach **Über**. Durch Öffnen des **Über**-Fensters wird automatisch ein Bedarf-Update angestoßen.

Das Update-Modul verbindet sich mit dem Bitdefender-Update-Server und sucht nach verfügbaren Updates.Wenn ein neues Update erkannt wird, wird es automatisch auf Ihren PC heruntergeladen und installiert.

Wichtig
Möglicherweise kann ein Neustart nach Abschluss des Updates notwendig werden. Wir empfehlen Ihnen, den Neustart möglichst zeitnah durchzuführen.

3.4. Wobei handelt es sich bei der Frequenz für automatische Updates?

Endpoint Security sucht automatisch nach Updates, wenn Sie Ihren Computer einschalten und dann jede **Stunde** danach erneut.

4. Die Quarantäne verwalten

Mit Bitdefender können Sie infizierte oder verdächtige Dateien in einem sicheren Bereich, der Quarantäne, isolieren. Befindet sich ein Virus in der Quarantäne, kann er keinen Schaden anrichten, da er nicht ausgeführt oder ausgelesen werden.

Sie können die **Quarantäne** über die Tafel **Sicherheit** aufrufen. Hier können Sie sich die Dateien in Quarantäne anzeigen lassen oder den Quarantäne-Ordner leeren.

4.1. Dateien in der Quarantäne anzeigen

Im Quarantäne-Bereich werden alle Dateien angezeigt, die momentan in der Quarantäne isoliert werden. Für jede Datei in Quarantäne werden der Name der erkannten Bedrohung, der Pfad zum ursprünglichen Speicherort und das Erkennungsdatum angezeigt.

Zum Anzeigen des Quarantäne-Ordners:

1. Doppelklicken Sie das BitDefender Icon in der Systembenachrichtung.
2. Gehen Sie zur Tafel **Sicherheit**.
3. Klicken Sie unten auf der Tafel auf die **Anzeigen**-Schaltfläche.

4.2. Dateien in der Quarantäne löschen

Zum Leeren des Quarantäne-Ordners:

1. Doppelklicken Sie das BitDefender Icon in der Systembenachrichtung.
2. Gehen Sie zur Tafel **Sicherheit**.
3. Klicken Sie unten auf der Tafel auf die **Leeren**-Schaltfläche.

4.3. Dateien aus der Quarantäne wiederherstellen

Zum Wiederherstellen einer Datei in Quarantäne:

1. Doppelklicken Sie das BitDefender Icon in der Systembenachrichtung.
2. Gehen Sie zur Tafel **Sicherheit**.
3. Klicken Sie unten auf der Tafel auf die **Anzeigen**-Schaltfläche.
4. Wählen Sie die Dateien aus, die Sie wiederherstellen möchten
5. Klicken Sie in der oberen rechten Bildschirmecke auf die **Wiederherstellen**-Schaltfläche.

5. Ereignisanzeige

Endpoint Security führt ein detailliertes Ereignisprotokoll über alle Aktivitäten der Software auf Ihrem Computer (einschließlich der Computer-Aktivitäten, die von der Inhaltssteuerung überwacht werden).Ereignisse sind ein wichtiges Hilfsmittel für die Überwachung Ihres Bitdefender-Schutzes.So können Sie beispielsweise einfach überprüfen ob das Update erfolgreich durchgeführt wurde, ob Malware auf Ihrem entdeckt wurde usw.

Um das Ereignisprotokoll aufzurufen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Endpoint Security-Fenster.
2. Gehen Sie zur Tafel **Ereignisse**.
3. Wählen Sie im zweiten Menü die Ereigniskategorie aus.Ereignisse sind in die folgenden Kategorien unterteilt:
   - **Malware-Schutz**
   - **Inhaltssteuerung**
   - **Update**
   - **Firewall**
   - **Allgemein**

Eine Liste von Ereignissen ist für jede Kategorie verfügbar.Um weitere Informationen über ein bestimmtes Ereignis in der Liste zu erhalten, müssen Sie nur darauf klicken. Details zu dem Ereignis werden in der unteren Hälfte des Fensters angezeigt.Sie erhalten die folgenden Informationen zu jedem Ereignis: eine Kurzbeschreibung; die Aktion, die Bitdefender für beim Auftreten des Ereignisses durchgeführt hat; das Datum und der Zeitpunkt des Ereignisses.

Sie können Ereignisse nach Ihrer Dringlichkeit ordnen.Es gibt drei Ereignistypen:

Information Diese Ereignisse weisen auf erfolgreich ausgeführte Vorgänge hin.

Warnung Diese Ereignisse weisen auf nicht-kritische Probleme hin.

Kritische Ereignisse weisen auf kritische Probleme hin.

Ereignisse können nur von Ihrem Netzwerkadministrator gelöscht werden.

6. Hilfe erhalten

Sollten Sie Probleme oder Fragen zu Endpoint Security haben, wenden Sie sich bitte an Ihren Netzwerkadministrator.

Um Produkt- und Kontaktinformationen zu finden, können Sie folgendermaßen vorgehen:

- Öffnen Sie das Endpoint Security-Fenster und klicken Sie in der unteren rechten Bildschirmecke auf das **Info**-Symbol.
- Klicken Sie mit der rechten Maustaste auf das Bitdefender-Symbol in der Task-Leiste und wählen Sie danach **Über**.